UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/591,708	06/09/2000	Stuart J. Jacobs	00-8010	2685

32127 7590 12/01/2005

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQE03H14
IRVING, TX 75038

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 12/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/591,708	JACOBS ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *19 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-22* is/are pending in the application.

4a) Of the above claim(s) *7 and 23* is/are ~~withdrawn from consideration~~ cancelled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-6 and 8-22 have been re-examined and are pending.

Claims 7 and 23 were cancelled.

2. This is a Final rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-6 and 8-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudia, et al. (US 5,825,880).

As per claim 1:

Sudia teaches in a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions comprising:

executing an application program at the node which is not highly secured; **[(col.3, lines 28-29 and col.7, lines 33-34); A "node which is**

not highly secured" can broadly interpret as a node that involves some kind of security which does not mean the node or the environment is unprotected. The limitation "is not highly secured" does not read the same as a node is not secured or unprotected. Additionally, even in applicant's own claim language where some form of security within the node is recited on lines 7-8, because of the cryptographic processing is involved.]

receiving an input requiring cryptographic-related processing; **(col.7, lines 12-13)**

generating a message via the application program based on the input **(col.7, lines 34-52)**, the message representing one of a predefined set of messages **(col.8, lines 10-11 and col.11, lines 6-15)** for processing by a cryptographic processing component **(col.9, lines 9-13)** located within the network node; **[(col.8, line 63 - col.9, line 23) Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device. This trusted device comprises a microchip that has a microcontroller for executing programs and a crypto-unit that performs encryption/decryption and signature processes (col.8, line 63 - col.9, line 23). Therefore, Sudia does teach executing the application program and cryptographic processing within the node.]**

transmitting the message to the cryptographic processing component; and **(col.7, lines 41-42)**

performing the cryptographic-related processing by the cryptographic processing component **(col.10, lines 5-46).**

As per claim 2:

Sudia discloses verifying a digital signature wherein includes encrypting and decrypting data (col.6, lines 32-42), retrieving the digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), and self-signed certificate processing (col.7, lines 45-52) within the node. Further, Sudia discloses certificate age checking in the form of time stamping (col.9, lines 13-16).

As per claim 3: See col.11, lines 9-22 and col.16, lines 35-67 discusses generating a function call message representing a request for performing a predetermined cryptographic related functions.

As per claim 4:

Sudia discloses generating an output message via the application program wherein the output message requiring cryptographic-related processing (col.11, lines 6-10), transmitting one of predefined the messages (col.11, lines 10-13) to the cryptographic processing component (col.9, lines 9-13) to perform the cryptographic-related processing (col.9, lines 55-56), and outputting the processed message (col.11, lines 17-18).

As per claim 5:

Sudia teaches a computer readable medium having stored thereon a plurality of sequences of instructions that may be invoked by a plurality of predefined messages executed by a processor in an

environment, which is not highly secure, cause said processor to perform a method comprising:

[(col.3, lines 28-29 and col.7, lines 33-34); A "node which is not highly secured" can broadly interpret as a node that involves some kind of security which does not mean the node or the environment is unprotected. The limitation "is not highly secured" does not read the same as a node is not secured or unprotected. Additionally, even in applicant's own claim language where some form of security within the node is recited on lines 7-8, because of the cryptographic processing is involved.]

receiving an input representing one of predefined messages; **(col.8, lines 10-11 and col.10, lines 10-14)**

transmitting, based on the input **(col.9, line 64 – col.10, lines 2)**, generating a function call message **(col.8, lines 24-55)** representing a request **(col.11, lines 6-9)** for performing a predetermined cryptographic related functions **(col.11, lines 9-22 and col.16, lines 35-67);** and

perform the cryptographic-related processing **(col.10, lines 15-30).**

As per claim 6:

Sudia discloses verifying a digital signature wherein includes encrypting and decrypting data (col.6, lines 32-42), retrieving the digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), and self-signed certificate processing (col.7, lines 45-52) within the node.

Further, Sudia discloses certificate age checking in the form of time stamping (col.9, lines 13-16).

As per claim 7: Cancelled

As per claim 8: See col.11, lines 6-13.

As per claim 9:

Sudia discloses in an environment which is not highly secure, a cryptographic module, comprising:

[(col.3, lines 28-29 and col.7, lines 33-34); A "node which is not highly secured" can broadly interpret as a node that involves some kind of security which does not mean the node or the environment is unprotected. The limitation "is not highly secured" does not read the same as a node is not secured or unprotected. Additionally, even in applicant's own claim language where some form of security within the node is recited on lines 7-8, because of the cryptographic processing is involved.]

a memory configured to operate within an environment **[(col.8, line 63 - col.9, line 23) Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device. This trusted device comprises a microchip that has a microcontroller for executing programs and a crypto-unit that performs encryption/decryption and signature processes (col.8, line 63 - col.9, line 23). Therefore, Sudia does teach executing the application program and cryptographic processing within the node.]** and to store a plurality of

cryptographic processing programs, each program being invoked via one of a plurality of predefined messages; and **(col.9, lines 3-18)**

a processor configured to operate within an environment and to: **(col.8, line 67 – col.9, line 2)**

receive an input requiring cryptographic-related processing, **(col.7, lines 34-40)**

generates one of predefined messages based on the input, **(col.8, lines 10-11 and col.10, lines 10-14)**

transmit the message to the first one of the cryptographic processing programs, and **(col.9, lines 55-56 and col.10, lines 15-30)**

to perform the cryptographic-related processing. **(col.11, lines 9-22 and col.16, lines 35-67)**

As per claim 10:

Sudia discloses verifying a digital signature wherein includes encrypting and decrypting data (col.6, lines 32-42), retrieving the digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), and self-signed certificate processing (col.7, lines 45-52) within the node. Further, Sudia discloses certificate age checking in the form of time stamping (col.9, lines 13-16).

As per claim 11: See col.7, lines 34-45; discussing transmit a function call to the first cryptographic processing program.

As per claim 12: See col.11, lines 6-13; discussing transmit the result of the cryptographic-related processing to an application program.

As per claim 13:

Sudia discusses in an environment which is not highly secure, a cryptographic module, comprising:

[(col.3, lines 28-29 and col.7, lines 33-34); A "node which is not highly secured" can broadly interpret as a node that involves some kind of security which does not mean the node or the environment is unprotected. The limitation "is not highly secured" does not read the same as a node is not secured or unprotected. Additionally, even in applicant's own claim language where some form of security within the node is recited on lines 7-8, because of the cryptographic processing is involved.]

means, operative in the environment **(col.6, lines 25-30)**, for storing a plurality of cryptographic processing programs that is invoked via one of the plurality of predefined messages; **(col.8, lines 10-11 and col.10, lines 10-14)**

means, operative in the environment, for receiving an input requiring cryptographic-related processing; **(col.7, lines 34-40)**

means, operative in the environment, for generating the one of predefined messages based on the input; **(col.8, lines 45-55)**

means, operative in the environment, for transmitting the message to the first one of the cryptographic processing programs, and **(col.9, lines 9-13)**

means, operative in the environment, for performing the cryptographic-related processing. **[(col.8, line 63 - col.9, line 23) Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device. This trusted device comprises a microchip that has a microcontroller for executing programs and a crypto-unit that performs encryption/decryption and signature processes (col.8, line 63 - col.9, line 23). Therefore, Sudia does teach executing the application program and cryptographic processing within the node.]**

As per claim 14:

Sudia discusses a method of performing cryptographic-related functions in a node coupled to other nodes in a network environment, which is not highly secure, the node includes an application program for handling communications with the other nodes the method comprising:

receiving in said node within the environment **(col.3, lines 28-29 and col.6, lines 22-30)** an input requiring cryptographic-related processing; **(col.7, lines 34-40 and lines 53-54)**

generating in said node within the environment a predefined message **(col.8, lines 10-11)** based on the input **(col.9, line 64 – col.10, lines 2)**, the message one of a plurality of predefined message usable by

of the cryptographic processing programs executed by the network node; **(col.9, lines 9-13 and lines 55-56)**

transmitting in said node within the environment a predefined message to the cryptographic processing program; **(col.10, lines 10-14)**

performing in said node within the environment, via cryptographic processing program the desired cryptographic-related operation. **(col.11, lines 9-22 and col.16, lines 35-67)**

[(col.8, line 63 - col.9, line 23) Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device. This trusted device comprises a microchip that has a microcontroller for executing programs and a crypto-unit that performs encryption/decryption and signature processes (col.8, line 63 - col.9, line 23). Therefore, Sudia does teach executing the application program and cryptographic processing within the node.]

As per claim 15: See col.11, lines 38-52.

As per claim 16:

Sudia discusses the method of requests for digital generation, verification, data encryption and decryption (col.6, lines 32-42), retrieval of digital certificate (col.10, lines 15-38), verifying the hierarchy (col.1, lines 24-38), self-signed certificate processing (col.7, lines 45-52), and certificate age checking in the form of time stamping (col.9, lines 13-16).

As per claim 17: See col.6, lines 4-19 and col. 7, lines 8-15; discussing the RSA signature scheme and the MD5 scheme.

As per claim 18: See col.6, lines 4-19 and col. 7, lines 8-15 ; discussing the RSA signature scheme and the MD5 scheme.

As per claim 19: See col.6, lines 4-19 and col. 7, lines 8-15; discussing the RSA signature scheme and the MD5 scheme.

As per claim 20: See col.6, lines 4-19 and col. 7, lines 8-15; discussing the RSA signature scheme and the MD5 scheme.

As per claim 21: See col.6, lines 24-30; discusses accessing a remote server via the network to retrieve cryptographic related information.

As per claim 22:

Sudia discloses a computer-readable medium that stores instructions executable by at least one processor in an environment which is not highly secure to perform a method for providing cryptographic-related functions, the method comprising:

[(col.3, lines 28-29 and col.7, lines 33-34); A "node which is not highly secured" can broadly interpret as a node that involves some kind of security which does not mean the node or the environment is unprotected. The limitation "is not highly secured" does not read the same as a node is not secured or unprotected. Additionally, even in applicant's own claim language where some form of security within the node is recited on lines 7-8, because of the cryptographic processing is involved.]

receiving in at least one processor in the environment **(col.3, lines 28-29 and col.7, lines 33-34)** a first function call from a predefined list

of function calls, the predefined list of function calls **(col.8, lines 10-11 and 11, lines 8-15)** representing available cryptographic-related functions executable by the at least one processor; **(col.8, line 62 – col.9, line 18)**

generating in at least one processor in the environment a request message based on the first function call **(col.7, lines 34-40)**, a for cryptographic processing to further transmit the request message representing a request for processing by **(col.11, lines 6-22 and col.16, lines 35-67)** a cryptographic processing module executed by the at least one processor; **(col.9, lines 9-18 and lines 55-56)**

transmitting in at least one processor in the environment the request message to the cryptographic processing module; and **(col.10, lines 10-38)**

performing in at least one processor in the environment the cryptographic-related processing. **[(col.8, line 63 - col.9, line 23) Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device. This trusted device comprises a microchip that has a microcontroller for executing programs and a crypto-unit that performs encryption/decryption and signature processes (col.8, line 63 - col.9, line 23). Therefore, Sudia does teach executing the application program and cryptographic processing within the node.]**

Response to Arguments

4. Applicant's arguments filed September 19, 2005 have been fully considered but they are not persuasive.

A) Claims 1-6 and 8-22 remains rejected under Sudia, et al. because the amended claims did not recite additional limitations that claims distinctive limitations from the previous rejections. The original claim 1 recites "which need not be highly secured" is no different from the amended limitation of "which is not highly secured" because both limitations still reads on executing the application program at the node which is not required to be highly secured but still secured. Thus, does not read on executing the application program on the node that is unsecured. By claiming the node is not highly secure could be given the broadest interpretation where it is according to one's perspective such that some or lower security or somewhat highly secure but not the maximum security can be interpreted as "is not highly secured". Additionally, even in applicant's own claim language where some form of security within the node is recited on lines 7-8, because of the cryptographic processing involved. It is inherent cryptographic processing serves the purpose to protect and secure the node or environment. How highly or not highly secure depends on the cryptographic process involving the type of algorithm used.

B) In response to applicant's arguments, the recitation "which is not highly secure" **has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).**

Claims 5, 9, 13, 14, and 22 have been amended only in the preamble where it does not further distinct within the claimed invention.

C) The argument in regards to the signing device is separate from the server. The applicant finds this argument irrelevant because applicant fails to explain the relevance of pointing out the server and the signing device is not on a single computer. Applicant argues that the claims read on executing an application program at the node and processing by the cryptographic processing component that is located within the node. Applicant's node is referred in Sudia as the trusted device which have the same general design as the smart card or the signing device (col.9, lines 22-24). This trusted device comprises a microchip that has a microcontroller for executing programs (col.8, line 63 - col.9, line 1) and the micro chip may also include a crypto-unit that

performs encryption/decryption and signature processes (col.9, lines 9-23). In addition, Sudia discloses the signing devices, which is also considered the trusted device as described above; encrypt their communications using a public/private cryptographic scheme (col.9, lines 55-56). Therefore, Sudia does teach executing the application program and cryptographic related processing within the node.

As per claim 5, there fails to have the limitation of cryptographic related processing in the node. It claims cryptographic related processing module executed by the processor (on lines 8-9).

As per claims 9, 13, and 22 fails to claims the limitation of cryptographic related processing in the node. These claims broadly claim cryptographic related processing (within or) "in the environment" rather than within the node as indicated by applicant's arguments. Having claimed in the environment broadly claims a large area and is not limited to just within the node or a particular area.

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100